Sub a4

WHAT IS CLAIMED IS:

1. A computer system comprising:

a processor;

an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;

an input device capable of being coupled to the processor, the input device being adapted to receive verification data, the verification data confirming authorized use of the access token;

a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:

an executable program code that accesses the access token and the verification data;

an executable program code that verifies validity of the access token using the verification data;

an executable program code that sets security policies in the processor; and

an executable program code that controls access to resources in the processor based on the security policies.

2. The computer system of claim 1 further comprising:

a nonvolatile storage device operably coupled to the processor;

a nonvolatile storage device access password that selectively allows access to the nonvolatile storage device, wherein the nonvolatile storage device password is supplied in response to the access token reading device reading an access token and the input device receiving verification data.

3. The computer system of claim 2, wherein at least one of the one or more policies is stored within the nonvolatile storage device password.

4. The computer system of claim 1, wherein at least one of the one or more policies is stored on the access token.

5. The computer system of claim 1 wherein one of the one or more policies corresponds to the verification data.

6. The computer system of claim 1 wherein one of the one or more policies includes BIOS control information that is used to configure the computer system.

7. The computer system of claim 6 wherein the BIOS control information further includes password change information, the password change information including one or more password change settings for a user using the one of the one or more policies.

8. The computer system of claim 1 further comprising a display device, wherein one of the one or more policies includes one or more interface settings that control a desktop presentation on the display device.

9. The computer system of claim 2 wherein a password corresponding to the nonvolatile storage device access password is stored on the access token.

10. The computer system of claim 2 wherein one or more bytes of the nonvolatile storage device access password are in a non-keyboard enterable format.

11. The computer system of claim 1 wherein the access token includes one or more bytes of data in a non-keyboard enterable format.

12. The computer system of claim 1 wherein the verification data includes biometric data supplied by a user.

13. The computer system of claim 1 wherein the input device includes a keyboard and the verification data includes a personal identification number.

14. A computer system comprising:

one or more processors;

memory electrically interconnected to the one or more processors;

an operating system for controlling the operation of the one or more processors;

an access token communication device electrically interconnected to at least one of the one or more processors;

an input device electrically interconnected to at least one of the one or more processors;

a nonvolatile storage device electrically interconnected to at least one of the one or more processors, the nonvolatile storage device including a nonvolatile memory;

one or more policies associated with the operating system;

wherein the operating system includes security code selectively enabled by the one or more policies to limit access to the computer system responsively to an access token read by the access token communication device.

15. The computer system of claim 14 wherein the access token further includes verification data, wherein the access token is read in response to the input device receiving authentication data corresponding to the verification data.

16. The computer system of claim 14 wherein the operating system includes a BIOS and wherein the BIOS is stored on nonvolatile memory that is electrically interconnected to the one or more processors.

17. The computer system of claim 14 wherein the access token communication device includes a smart card communication device.

18. The computer system of claim 14 wherein the access token communication device includes network circuitry that is adapted to receive signals from one or more computers interconnected on a computer network.

19. The computer system of claim 14 wherein the access token communication device includes a modem that receives signals from a communications line.

20. The computer system of claim 14 wherein the input device is a keyboard.

21. The computer system of claim 14 wherein the input device includes a biometric data reading device.

22. The computer system of claim 14 wherein the biometric data reading device includes a fingerprint scanner.

23. The computer system of claim 14 wherein the biometric data reading device includes a retinal scanning device.

24. The computer system of claim 14 wherein the nonvolatile storage device includes a hard disk drive.

25. The computer system of claim 14 further comprising a data access code stored in the nonvolatile memory, wherein a data request code corresponding to the data access code alters a state of the nonvolatile storage device.

26. A method for manufacturing a computer system, said method comprising:
providing a computer system, the computer system including:
one or more processors;
memory operably coupled to the one or more processors;
one or more images of an operating system for controlling the operation of the one or more processors;

an access token reading device that is adapted to read an access token;

an input device that is adapted to receive verification data, the verification data confirming authorized use of the access token;

a nonvolatile storage device operably coupled to the memory;

a nonvolatile storage device access password that selectively allows access to the nonvolatile storage device, wherein the nonvolatile storage device password is supplied in response to the access token reading device reading an access token and the input device receiving verification data;

storing a master password on the access token; and

storing a nonvolatile storage device password on the access token.

27. The method of claim 26 further comprising:

storing a password corresponding to the nonvolatile storage device password on the nonvolatile storage device.

28. A method for protecting information stored in an information handling system, said method comprising:

reading an access token;

verifying the validity of the access token;

setting security policies in the information handling system;

unlocking a nonvolatile storage device on the information handling system.

29. A method for assembling a computer system, said method comprising:

receiving a list of components for assembling the computer system;

receiving one or more security policies; and

configuring the computer system using the one or more security policies.

30. The method of claim 29 further comprising:
initializing a system password installed on the computer system.

31. The method of claim 29 further comprising:
providing a nonvolatile storage device for the computer system,
wherein the nonvolatile storage device includes a nonvolatile storage device password; and
initializing the nonvolatile storage device password.

32. The method of claim 29 wherein the configuring includes modifying a nonvolatile memory installed in the computer system.

33. The method of claim 29 further comprising:
retaining a copy of the nonvolatile storage device password at a location removed from the computer system.

34. The method of claim 29 further comprising:
preparing an access token for the computer system.

35. A method of using an access token, said method comprising:
transferring one or more passwords from the access token to a computer system.

36. The method of claim 35 wherein the transferring is in response to an access code received by the access token.

37. The method of claim 35 wherein one of the one or more passwords corresponds to a computer system password installed on the computer system.

38. The method of claim 35 wherein one of the one or more passwords corresponds to a nonvolatile storage device password installed on a nonvolatile storage device.

39. The method of claim 35 wherein the access token.

40. An access token for use with a computer system, said access token comprising:

one or more security policies adapted to be used by a computer system, wherein the one or more security policies are stored in an encrypted format; and

an access code stored on the access token, wherein the access token transmits the one or more security policies in response to receiving a data stream corresponding to the access code.

41. A computer operable medium for protecting a computer system, said computer operable medium comprising:

means for reading an access token;

means for verifying the validity of the access token;

means for setting security policies in the information handling system; and

means for unlocking a nonvolatile storage device on the information handling system.

42. An information handling system comprising:

means for reading an access token;

means for verifying the validity of the access token;

means for setting security policies in the information handling system; and

means for unlocking a nonvolatile storage device on the information handling system.